CARDINALOPS

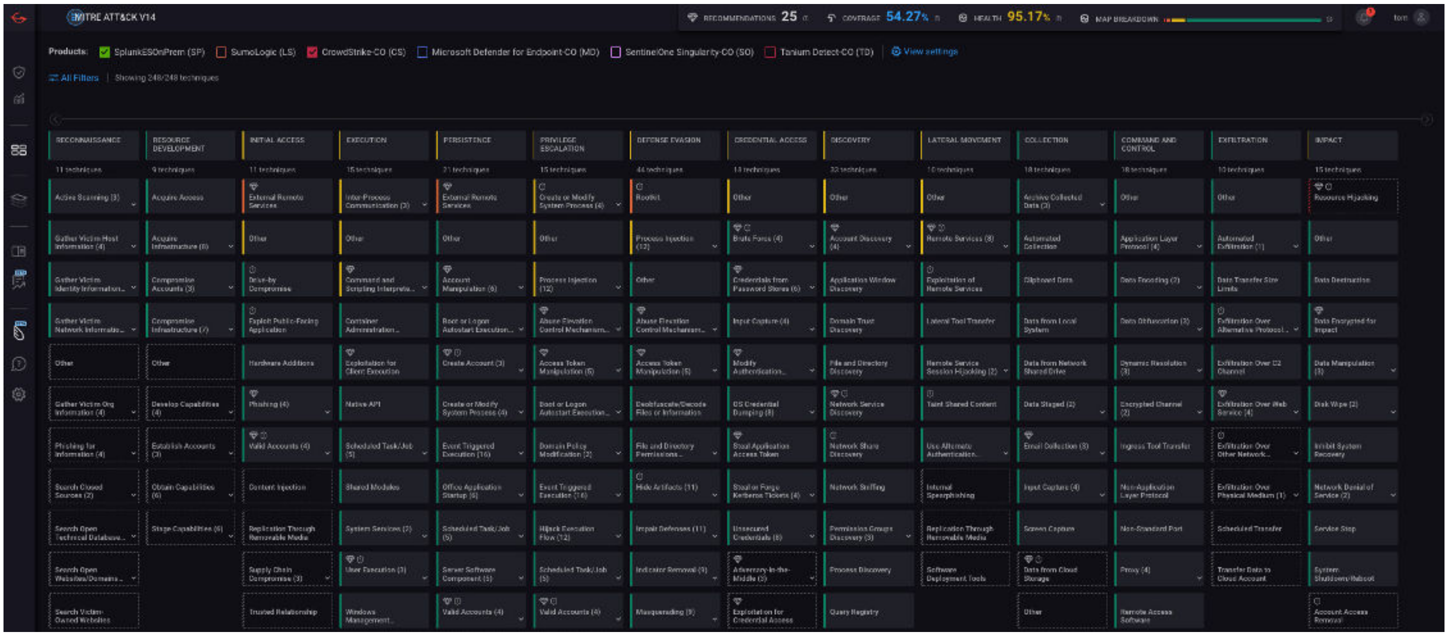
Detection Posture Management

Strengthen the Detection Posture of Your Existing SOC Tools

Detect the threats that matter most. Always.

Detection tools, such as SIEM, still serve as the operating system of most SOCs. And although they are capable of providing comprehensive threat coverage, security teams struggle to develop and implement enough new detections to keep up with emerging threats and lack the resources and capability to audit their existing rules for misconfigurations or excess noise. This means your detection stack is not optimized to cover the highest-priority MITRE ATT&CK techniques relevant to your organization. These implementation and maintenance gaps have remained difficult for detection engineers to manage and leave enterprises exposed to a large array of attacks without any visibility into their detection posture.

Eliminate Detection Coverage Gaps with Automation and MITRE ATT&CK



MITRE ATT&CK V14

RECOMMENDATIONS 25 | COVERAGE 54.27% | HEALTH 95.17% | MAP BREAKDOWN

Products: ☑ SplunkESOnPrem (SP) □ SumoLogic (LS) ☑ CrowdStrike-CO (CS) □ Microsoft Defender for Endpoint-CO (MD) □ SentinelOne Singularity-CO (SO) □ Tanium Detect-CO (TD) | View settings

All Filters | Showing 248/248 techniques

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
11 techniques	9 techniques	11 techniques	15 techniques	21 techniques	15 techniques	44 techniques	14 techniques	32 techniques	10 techniques	18 techniques	18 techniques	10 techniques	15 techniques
Active Scanning (3)	Acquire Access	External Remote Services	Inter-Process Communication (3)	External Remote Services	Create or Modify System Process (4)	Rootkit	Other	Other	Other	Archive Collected Data (3)	Other	Other	Resource Hijacking
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Other	Other	Other	Other	Process Injection (12)	Brute Force (4)	Account Discovery (4)	Remote Services (8)	Automated Collection	Application Layer Protocol (4)	Automated Exfiltration (1)	Other
Gather Victim Identity Information...	Compromise Accounts (3)	Drive-by Compromise	Command and Scripting Interprete...	Account Manipulation (6)	Process Injection (12)	Other	Credentials from Password Stores (6)	Application Window Discovery	Exploitation of Remote Services	Clipboard Data	Data Encoding (2)	Data Transfer Size Limits	Data Destruction
Gather Victim Network Informatio...	Compromise Infrastructure (7)	Exploit Public-Facing Application	Container Administration...	Boot or Logon Autostart Execution...	Abuse Elevation Control Mechanism...	Abuse Elevation Control Mechanism...	Input Capture (4)	Domain Trust Discovery	Lateral Tool Transfer	Data from Local System	Data Obfuscation (3)	Exfiltration Over Alternative Protocol...	Data Encrypted for Impact
Other	Other	Hardware Additions	Exploitation for Client Execution	Create Account (3)	Access Token Manipulation (5)	Access Token Manipulation (5)	Modify Authentication...	File and Directory Discovery	Remote Service Session Hijacking (2)	Data from Network Shared Drive	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (4)	Native API	Create or Modify System Process (4)	Boot or Logon Autostart Execution...	Deobfuscate/Decode Files or Information	OS Credential Dumping (8)	Network Service Discovery	Taint Shared Content	Data Staged (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Valid Accounts (4)	Scheduled Task/Job (5)	Event Triggered Execution (16)	Domain Policy Modification (2)	File and Directory Permissions...	Steal Application Access Token	Network Share Discovery	Use Alternate Authentication...	Email Collection (3)	Ingress Tool Transfer	Exfiltration Over Other Network...	Inhibit System Recovery
Search Closed Sources (2)	Obtain Capabilities (6)	Content Injection	Shared Modules	Office Application Startup (6)	Event Triggered Execution (16)	Hide Artifacts (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing	Internal Spearphishing	Input Capture (4)	Non-Application Layer Protocol	Exfiltration Over Physical Medium (1)	Network Denial of Service (2)
Search Open Technical Database...	Stage Capabilities (6)	Replication Through Removable Media	System Services (2)	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Impair Defenses (11)	Unsecured Credentials (8)	Permission Groups Discovery (3)	Replication Through Removable Media	Screen Capture	Non-Standard Port	Scheduled Transfer	Service Stop
Search Open Websites/Domains...		Supply Chain Compromise (3)	User Execution (3)	Server Software Component (5)	Scheduled Task/Job (5)	Indicator Removal (9)	Adversary-in-the-Middle (3)	Process Discovery	Software Deployment Tools	Data from Cloud Storage	Proxy (4)	Transfer Data to Cloud Account	System Shutdown/Reboot
Search Victim-Owned Websites		Trusted Relationship	Windows Management...	Valid Accounts (4)	Valid Accounts (4)	Masquerading (9)	Exploitation for Credential Access	Query Registry		Other	Remote Access Software		Account Access Removal

Increase the Effectiveness of Your Existing Security Stack and Team

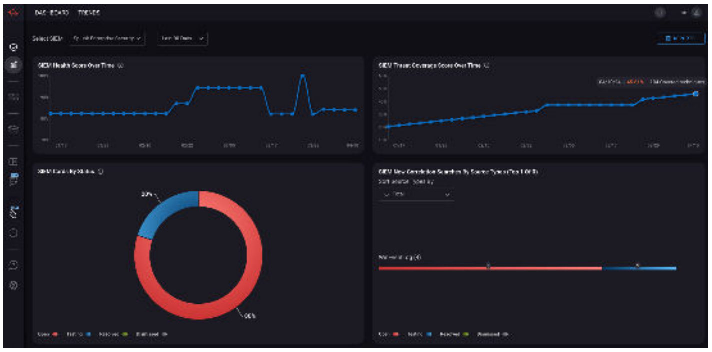
- Map current detection coverage to MITRE ATT&CK for continuous visibility
- Automatically detect and fix broken, misconfigured, and noisy rules
- Receive new, deployment-ready rules and recommendations for the threats relevant to you
- Automate manual tasks to free up team members to perform high-value work

Integrations

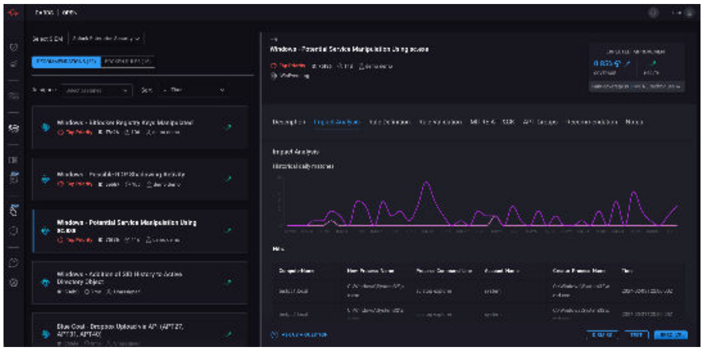
splunk> CROWDSTRIKE Chronicle part of Google Cloud Microsoft Sentinel IBM QRadar

Proactively Assess and Strengthen the Detection Coverage of your Existing Tools

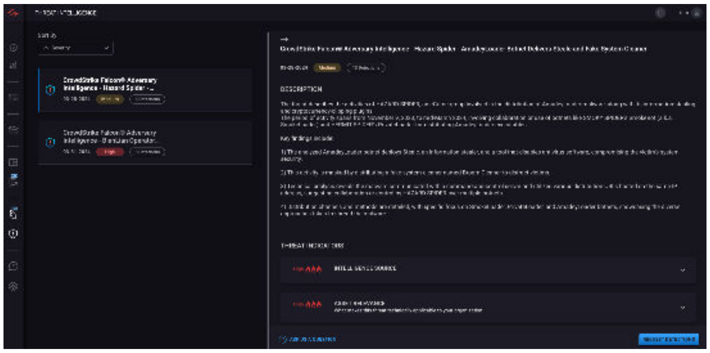
Report Trends and Track Improvement



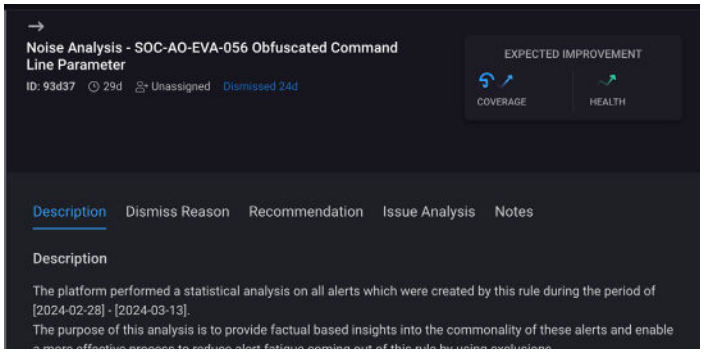
Receive New Rule Recommendations



Operationalize Threat Intelligence



Analyze and Tune Noisy Rules



Noise Analysis - SOC-AO-EVA-056 Obfuscated Command Line Parameter

ID: 93d37 29d Unassigned Dismissed 24d

Description

The platform performed a statistical analysis on all alerts which were created by this rule during the period of [2024-02-28] - [2024-03-13].
The purpose of this analysis is to provide factual based insights into the commonality of these alerts and enable a more effective process to reduce alert fatigue coming out of this rule by using exclusions.

Challenges CardinalOps Addresses

- How do we continuously improve our detection posture to reduce risk?
- Are we missing detections for the MITRE ATT&CK techniques and adversaries most relevant to our business?
- Do we have detection rules that are broken due to ongoing changes in our infrastructure – creating additional gaps for attackers?
- How do we quickly onboard new detections for new log sources (AWS, Azure, GCP, Wiz, etc.) and high-profile vulnerabilities (log4j, Follina, etc.)?
- How do we report our detection posture to the business and other teams using standard metrics and heatmaps?

About CardinalOps

Powered by automation and MITRE ATT&CK, the CardinalOps platform continuously assesses and strengthens the detection coverage of your existing SIEM and detection tools so you can detect the threats that matter most. Always. Native API-driven integrations include Splunk, Microsoft Sentinel, IBM QRadar, Google Chronicle, and CrowdStrike.

CARDINALOPS
Detection Posture Management

To learn more, visit **www.cardinalops.com**